ПАМЯТКА
по безопасности при использовании удаленных каналов обслуживания
АКБ «Ланта-Банк» (АО)

1.Общие положения

Вы присоединились к Договору, в рамках которого клиентам Банка предоставляется возможность совершать операции и получать информацию по счетам через **Удалённые каналы обслуживания**, к которым относятся:

1) Устройства самообслуживания Банка;
2) системы ДБО Faktura/iBank2;
3) Мобильный банк;
4) Контактный Центр Банка.

Вы имеете возможность установить ограничение доступности (видимости) счетов, которые Вы не хотите использовать в Удалённых каналах обслуживания. Ограничение можно установить отдельно для каждого из Удалённых каналов: для Устройств самообслуживания Банка, для систем ДБО Faktura/iBank2 и Мобильного банка.

Установить или изменить перечень доступных счетов Вы можете как через системы ДБО Faktura/iBank2 (по всем счетам), так и в любом подразделении Банка на территории обслуживания Договора (только по счетам вкладов).

Правила пользования Удалёнными каналами обслуживания определены в Договоре.

Использование Удалённых каналов обслуживания сопряжено с риском получения неуполномоченными лицами несанкционированного доступа к конфиденциальной информации Клиента и осуществления переводов денежных средств с его счетов.

К **конфиденциальной информации** Клиента относится:

- информация об остатках денежных средств на счетах;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных Вами распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами, в том числе данные Держателей карт;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

Ниже приведены рекомендуемые Банком меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации Клиента.

Помните! Передача карты или ее реквизитов, Логина (Идентификатора пользователя), Постоянного пароля, Одноразовых паролей, Контрольной информации и Кода клиента, предназначенных для доступа и подтверждения операций в Удалённых каналах обслуживания, другому лицу (в том числе работнику Банка) предоставляет другим лицам возможность проводить операции по Вашим счетам.

При любых подозрениях на мошенничество (если Вы получили SMS-сообщение/Push-уведомление от Банка по операции, которую Вы не совершали, или оно вызывает любые сомнения и опасения), следует незамедлительно обратиться в Контактный Центр Банка по номерам телефонов, указанным на оборотной стороне карты и на официальном сайте Банка:

+7 (495) 785-15-15
+7 (800) 200-30-22

2. Меры безопасности при использовании карты

Храните свою карту в недоступном для окружающих месте. Не передавайте карту и/или её реквизиты другому лицу. Рекомендуется хранить карту отдельно от наличных денег и документов, удостоверяющих личность, особенно в поездках.

Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.

Не следуйте советам и просьбам третьих лиц, не принимайте их помощь при проведении операций и не проводите операции со своей карты на указанные ими реквизиты. При

необходимости обратитесь к сотрудникам в подразделении Банка или позвоните по номерам телефонов, указанным на Устройстве самообслуживания или на оборотной стороне Вашей карты.

Во избежание использования Вашей карты третьим лицом храните ПИН отдельно от карты, исключив одновременный доступ к ним (например, при хранении в одном бумажнике), не пишите ПИН на карте, не сообщайте ПИН другим лицам (в том числе родственникам), не вводите ПИН при работе в сети Интернет.

Ни при каких обстоятельствах не сообщайте свой ПИН никому, включая сотрудников Банка.

3. Меры безопасности при работе в системах ДБО Faktura/iBank2

Для входа в системы ДБО Faktura/iBank2 Вам необходимо ввести Логин (Идентификатор пользователя) и Постоянный пароль, дополнительно может вводиться Одноразовый пароль (если данная опция предусмотрена Вами при настройке Личного кабинета). Для входа в системы ДБО Faktura/iBank2 не требуется вводить никакой другой информации.

Внимание! Если для входа в системы ДБО Faktura/iBank2 Вам предлагается ввести любую другую конфиденциальную информацию или дополнительные данные (номера карт, номер мобильного телефона, Контрольную информацию или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы на сайте системы ДБО Faktura/iBank2 и срочно обратиться в Банк.

Банк никогда не запрашивает пароли для отмены операций или шаблонов в системах ДБО Faktura/iBank2. Если Вам предлагается ввести пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы на сайте системы ДБО Faktura/iBank2 и срочно обратиться в Банк.

При получении от Банка на мобильное устройство SMS-сообщения и/или Push-уведомления с Одноразовым паролем внимательно ознакомьтесь с информацией в сообщении/уведомлении: все реквизиты операции в направленном Вам сообщении/уведомлении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом SMS-сообщении/Push-уведомлении корректна, можно вводить пароль.

Помните! Вводя Одноразовый пароль, Вы даёте Банку распоряжение о проведении операции в соответствии с реквизитами, указанными в SMS-сообщении/Push-уведомлении.

Ни при каких обстоятельствах не сообщайте Постоянный и Одноразовые пароли никому, включая сотрудников Банка.

Избегайте использования сетей Wi-Fi для работы в системах ДБО Faktura/iBank2. В случае использования сетей Wi-Fi, используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашей конфиденциальной информации.

В случае утраты или кражи носителей с Логином (Идентификатором пользователя) и Постоянным паролем Вам следует незамедлительно обратиться в Контактный Центр Банка.

При работе в системах ДБО Faktura/iBank2 всегда проверяйте, что установлено защищённое ssl-соединение с официальными сайтами по протоколу http**s** (**https**://elf.faktura.ru/elf/app/, **https**://ibank2.lanta.ru/ibank2/#/). В адресной строке окна браузера должен быть символ замка, обозначающий наличие защищённого соединения, которое может незначительно отличаться в зависимости от браузера. Например, в браузере Microsoft Internet Explorer в правой части адресной строки должен отображаться жёлтый замок.

Не пользуйтесь системами ДБО Faktura/iBank2 через мобильное устройство, особенно через устройство, на которое приходят SMS-сообщения/Push-уведомления с подтверждающим Одноразовым паролем. Для мобильных устройств существуют специально разработанные Банком мобильные приложения. Получить информацию о таких мобильных приложениях Банка и способах их установки Вы можете на официальном сайте Банка.

Для исключения компрометации Вашей финансовой информации и хищения средств, настоятельно не рекомендуем Вам подключать к услугам Банка номера телефонов, которые Вам не принадлежат, а также использовать sim-карты, купленные вне салонов связи (с рук).

Пользуйтесь дополнительными возможностями систем ДБО Faktura/iBank2 по повышению уровня безопасности (SMS-информирование/Push-уведомления о входе в системы ДБО Faktura/iBank2, настройка видимости карт и пр.).

Не устанавливайте на мобильное устройство, на которое Банк отправляет SMS-сообщения/Push-уведомления с подтверждающими Одноразовыми паролями, приложения неизвестных издателей, в том числе полученные по ссылкам от неизвестных Вам источников.

Помните, что Банк не рассылает своим клиентам ссылки или указания на установку мобильных приложений через сообщения SMS/Push/MMS/e-mail.

На мобильных устройствах, которые Вы используете для доступа к системам ДБО Faktura/iBank2:

- используйте лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением;
- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем мобильного устройства;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты Вашего мобильного устройства.

Завершение работы с системами ДБО Faktura/iBank2 выполняйте путем выбора соответствующего пункта меню (кнопка «Выход»).

4. Меры безопасности при работе с Устройствами самообслуживания

При проведении операции с вводом ПИНа ВСЕГДА прикрывайте клавиатуру, например, свободной рукой. Это не позволит мошенникам увидеть Ваш ПИН или записать его на видеокамеру.

Электронные замки доступа по картам в специальные помещения, где устанавливаются Устройства самообслуживания, не должны требовать ввода ПИНа. Если для прохода в помещение от Вас требуется ввести ПИН, не делая этого, обратитесь в Банк. Если Вы ранее пытались воспользоваться подобным устройством, рекомендуем Вам незамедлительно заблокировать карту, позвонив по номерам телефонов, указанным на Устройстве самообслуживания или на оборотной стороне Вашей карты, обратившись в Контактный центра Банка, независимо от того, получили ли Вы доступ к устройству или нет.

До проведения операции в Устройстве самообслуживания осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств, следует незамедлительно сообщить об этом по номерам телефонов, указанным на Устройстве самообслуживания или на оборотной стороне Вашей карты. Операцию с использованием карты для получения наличных в данном Устройстве самообслуживания проводить не следует.

Не применяйте физическую силу, чтобы вставить карту в Устройство самообслуживания. Если карта не вставляется, воздержитесь от использования данного Устройства самообслуживания.

При приёме и возврате карты банкоматом не пытайтесь ускорить прерывистое движение карты в картоприёмнике. Неравномерное движение карты является не сбоем, а необходимым средством защиты Вашей карты от компрометации.

Внимание! Не совершайте на Устройстве самообслуживания никаких операций по указаниям посторонних лиц, в том числе позвонивших Вам и представившихся работниками Банка или других организаций.

5. Меры безопасности при работе с Мобильным банком и Мобильными приложениями Банка

При утрате Мобильного устройства, к которому подключен Мобильный банк или на которое установлено Мобильное приложение Банка, Вам следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для приостановки действия Мобильного банка и/или блокировки доступа в системы ДБО Faktura/iBank2.

При смене номера телефона, на который подключен Мобильный банк, Вам необходимо незамедлительно обратиться в любое подразделение Банка и оформить заявление на отключение Мобильного банка от старого номера телефона и на подключение услуги на новый номер телефона.

При внезапном прекращении работы SIM-карты необходимо срочно обратиться к своему оператору сотовой связи за уточнением причин – в отношении Вас возможно проведение мошеннических действий третьими лицами.

Будьте внимательны – не оставляйте свое Мобильное устройство без присмотра, чтобы исключить несанкционированное использование Мобильного банка и мобильных приложений Банка.

Используйте только официальные мобильные приложения Банка, доступные в официальных магазинах приложений производителей мобильных платформ.

Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваше мобильное устройство. Используйте лицензированное антивирусное программное обеспечение для мобильного устройства, регулярно осуществляйте обновление антивирусных баз (по возможности, в автоматическом режиме) и выполняйте полную проверку устройства.

Не устанавливайте на свое мобильное устройство нелицензионные операционные системы и приложения, так как это отключает защитные механизмы, заложенные производителем мобильной платформы и Вашего устройства. В результате Ваше мобильное устройство становится уязвимым к заражению вредоносными программами.

Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Банка.

Установите на Вашем мобильном устройстве пароль блокировки экрана и доступа к устройству (данная возможность доступна для любых современных моделей мобильных устройств).

Избегайте использования мобильного устройства для доступа к полнофункциональной версии систем ДБО Faktura/iBank2, для этого существуют специализированные мобильные приложения, разработанные Банком.

Завершайте работу с мобильными приложениями Банка через завершение сессии (кнопка «Выход»).

6. Защита от SMS/Push-мошенничества

Мошеннические SMS-сообщения/Push-уведомления, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS-сообщении/Push-уведомлении номер телефона для уточнения информации. Перезвонившему Клиенту мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки банка и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и тому подобное, в зависимости от содержания SMS-сообщения/Push-уведомления.

В случае получения подобных SMS-сообщений/Push-уведомлений категорически запрещено:

- перезванивать на номер телефона, указанный в SMS-сообщении/Push-уведомлении;
- предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИНе, CVV2/CVC2/ППК2 коде), Контрольной информации, Коде клиента Логине (Идентификаторе пользователя), Постоянном пароле, Одноразовых паролях, в том числе посредством направления ответных SMS-сообщений/Push-уведомлений;
- проводить через Устройства самообслуживания какие-либо операции по инструкциям, полученным в SMS-сообщении/Push-уведомлении.

В случаях, когда Банк рассылает информационные SMS-сообщения/Push-уведомления:

- в SMS-сообщениях/Push-уведомлениях, направленных Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты в формате *XXXX (мошенникам они не известны);
- в SMS-сообщениях/Push-уведомлениях Банка всегда указываются только официальные номера телефонов Банка, опубликованные на официальном сайте Банка или указанные на Вашей банковской карте;

- SMS-сообщения/Push-уведомления Банка не рассылаются с официальных номеров телефонов Контактного Центра Банка +7(495) 785-15-15 и +7(800) 200-30-22.

Если полученное SMS-сообщение/Push-уведомление вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Банка по официальным номерам телефонов, размещенным на оборотной стороне карты или на официальном сайте Банка.

В случае если Вы все же пострадали от SMS/Push-мошенничества, необходимо:

- немедленно обратиться в Контактный Центр Банка по официальным номерам телефонов и заблокировать карту, реквизиты которой были сообщены мошенникам или по которой были совершены мошеннические операции;

- в случае мошеннического перевода денежных средств на номер сотового оператора немедленно обратиться по телефону к соответствующему оператору связи, в адрес которого переведены средства, с заявлением о мошенничестве и возврате средств (информация о сотовом операторе и номере телефона контактного центра указана на чеке о совершенном переводе);

- подать заявление о совершённом мошенничестве через любое подразделение полиции.

7. Защита от e-mail мошенничества

Массовые мошеннические e-mail-рассылки, маскируясь под бренд АКБ «Ланта-Банк» (АО), как правило, предназначены для:

- заманивания получателей сообщений на сайты-«ловушки», на которых под различными предлогами мошенники попытаются получить Вашу конфиденциальную информацию (персональные данные, Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информация, номера банковских карт и их сроки действия, ПИНы, CVV2/CVC2/ППК2 коды, Код клиента и иную информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц;

- принуждения получателей писем под различными предлогами на открытие вложенных файлов, содержащих вирус, или переход по ссылке для загрузки вирусного файла.

Признаки того, что e-mail-сообщение является мошенническим:

- сообщения замаскированы под официальные письма Банка и требуют от Вас каких-либо быстрых действий или ответа;

- адрес отправителя и тема сообщения замаскированы под обращения от имени Банка. Примеры мошеннических сообщений: отправитель: Ланта Банк Онлайн (info@lantabank.ru) тема: «Сообщение об образовании задолженности»; отправитель: Ланта Банк (noreply@lanta.com) тема: «Сообщение о просроченной задолженности»; отправитель: Ланта Информ (statistics@bank-lanta.info) тема: «Сообщение о состоянии просроченной задолженности на ДД.ММ.ГГГГ»;

- письма содержат ссылки на интернет-ресурсы, похожие на официальные ресурсы Банка;

- URL-адрес ссылки в письме отличается от официального адреса (www.lanta.ru), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Вашей конфиденциальной информации (персональных данных);

- к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть;

- в тексте содержатся явные опечатки или орфографические ошибки.

Обращаем Ваше внимание, что АКБ «Ланта-Банк» (АО) никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить конфиденциальную информацию (персональные данные, Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера банковских карт и сроки их действия, ПИНы, CVV2/CVC2/ППК2 коды, Код клиента, данные документа, удостоверяющего личность, номер мобильного телефона и иную информацию);

- не отправляет сообщения с формой для ввода Вашей конфиденциальной информации (персональных данных);

- не просит Вас зайти в личный кабинет систем ДБО Faktura/iBank2 по ссылкам в письмах.

+7 (495) 785-15-15
+7 (800) 200-30-22